UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/579,628	05/17/2006	Yibo Zhang	2006_0718A	9174

52349 7590 03/09/2009

WENDEROTH, LIND & PONACK L.L.P.
1030 15th Street, N.W.
Suite 400 East
Washington, DC 20005-1503

EXAMINER	
CHAI, LONGBIT	

ART UNIT	PAPER NUMBER
2431	

MAIL DATE	DELIVERY MODE
03/09/2009	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/579,628	ZHANG ET AL.	
	Examiner	Art Unit	
	LONGBIT CHAI	2431	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *21 January 2009*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1,2 and 11-26* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1,2 and 11-26* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *17 May 2006* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. Currently pending claims are 1, 2 and 11 – 26.

Response to Arguments

2. Applicant's arguments with respect to instant claims have been fully considered but are moot in view of the new ground(s) of rejection necessitated by Applicant's amendment.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

3. Claims 1 and 15 are rejected under 35 U.S.C. 103(a) as being unpatentable over Tetsuya et al. (JP 2002-026899), in view of Cho (KR 2003-005604).

Tetsuya teaches a communication device requested for authentication for connection from another communication device, the communication device comprising:

a receiving section for receiving, from the another communication device, an authentication request including device information by which the another communication device is capable of uniquely being determined to be a source, and for monitoring and determining whether or not the authentication request is changed by an unspecified third party while being transmitted (Tetsuya: Para [0036] Line 1 – 4 and Para

[0012] Line 8 – 10: (a) a public key is qualified as a part of device information and (b) a data integrity was verified and assured w/o altering the data).

However, Tetsuya does not disclose expressly monitoring and determining whether or not the authentication request is changed during the transmission.

Cho teaches monitoring and determining whether or not the authentication request is changed during the transmission (Cho: DESCRIPTION / Line 1 – 13: providing a signature for an authentication request message that can be monitored and tested by the receiver to assure the message data integrity).

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Cho within the system of Tetsuya because (a) Tetsuya teaches providing a communication authentication means that assures a data integrity was verified and assured w/o altering the data (Tetsuya: Para [0036] Line 1 – 4 and Para [0012] Line 8 – 10), and (b) Cho teaches a specific security enhanced mechanism by providing a signature for an authentication request message that can be monitored and tested by the receiver to assure the message data integrity (Cho: DESCRIPTION / Line 1 – 13).

a display section for, when it is determined that the authentication request is not changed, displaying the device information included in the authentication request on a screen thereof (Tetsuya: Para [0015]: outputting visual / display @ verification data);

an input section for receiving an input of a confirmation result of the displayed device information from a user; a transmission section for transmitting an authentication response including information indicative of verification or non-verification of the authentication with the another communication device in accordance with the result input to the input section (Tetsuya: Para [0014] Line 7 – 9: a user input of confirmation / judgment of matching verification data); and

an authentication section for when the information included in the authentication response is indicative of verification of the authentication, performing key exchange with the another communication device using the device information included in the authentication request and the information included in the authentication response (Tetsuya: Para [0036] Line 13 – 24: using the public key information included in the authentication request and the random value included in the authentication response message to generate a common encryption / decryption key).

As per claim 15, Tetsuya as modified teaches wherein the display section further displays channel information used for reception of the authentication request, in addition to the device information included in the authentication request, thereby making it possible for the user to determine whether or not the authentication request is transferred using another channel by the unspecified third party (Tetsuya: Para [0036] Line 11 – 12) & (Cho: DESCRIPTION / Line 1 – 13).

4. Claim 17 is rejected under 35 U.S.C. 103(a) as being unpatentable over Tetsuya et al. (JP 2002-026899), in view of Cho (KR 2003-005604), and in view of Briscoe et al. (U.S. Patent 7,464,402).

As per claim 17, Tetsuya as modified teaches whether or not a public key and a signature in the device information included in the authentication request are changed, whether or not the received authentication request is changed by the unspecified third party (Tetsuya: Para [0036] Line 11 – 12) & (Cho: DESCRIPTION / Line 1 – 13).

However, Tetsuya as modified does not disclose expressly the user is able to determine, based on whether or not the authentication request is received a plurality of times.

Briscoe teaches the user is able to determine, based on whether or not the authentication request is received a plurality of times (Briscoe: Column 7 Line 46 – 48: detect the security against flooding of the network messages).

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Briscoe within the system of Tetsuya as modified because (a) Tetsuya teaches providing a communication authentication means that assures a data integrity was verified and assured w/o altering the data (Tetsuya: Para [0036] Line 1 – 4 and Para [0012] Line 8 – 10), and (b) Briscoe teaches an enhanced security mechanism of detecting the security against flooding of the network messages (Briscoe: Column 7 Line 46 – 48: detect the security against flooding of the network messages).

5. Claims 2 and 16 are rejected under 35 U.S.C. 103(a) as being unpatentable over Kang et al. (U.S. Patent 7,096,352), in view of Kimura (U.S. Patent 2001/0048744).

As per claim 2, kang teaches a communication device requesting another communication device for authentication for connection, the communication device comprising:

a transmission section for transmitting an authentication request including device information indicative of the communication device to the another communication device (Kang: Column 3 Line 1 – 20: the “random” value data field @ CilentHello message, that makes authentication request, uniquely identify a particular requesting device);

a receiving section for receiving, from another communication device, an authentication response corresponding to the authentication request and including

device information by which the another communication device is capable of being determined to be a source, and for monitoring and determining whether or not the authentication response is changed by an unspecified third party while being transmitted (Kang: Column 3 Line 18 – 27, Column 1 Line 49 – 51 and Column 4 Line 35 – 38: (a) the receiving device generates a specific server random value, that uniquely identify a particular response device, in response to the received random valued from the sending device, on a mutual authentication basis to prove that both devices indeed computes the same security parameters and (b) a simple ***hash value*** is used for assuring message data integrity (i.e. data is not altered) by using a simple public key).

However, Kang does not disclose expressly, when it is determined that the authentication response is not changed, a display section for displaying the device information included in the authentication response on a screen.

Kimura teaches **when it is determined that the authentication response is not changed, a display section for displaying the device information included in the authentication response on a screen n thereof** (Kang: Column 3 Line 18 – 27 and Column 1 Line 49 – 51) & (Kimura: Para [0056] and Para [0006]: (a) the access point device allows the user to see / view who is making the request before granting authorization, instead of transparently using automatic authorization (b) though the message is an authentication response message from the server; however, in fact, this message is also an authentication request message in correspondence with "mutual authentication" that requires the receiver authentication to the sender device).

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Kimura within the system of Kang because (a) Kang teaches a mutual authentication (co-equal) mechanism between a sender and a receiver

(i.e. a client and the server) and allowing a challenge request of receiver authentication to the sender (Kang: Column 2 Line 64 – 65, Column 2 Line 60 – 62 and Column 1 Line 49 – 51) and (b) Kimura teaches a method that can provide a significantly improvement of security level by allowing the user to see / view who is making the request before granting authorization, instead of transparently using automatic authorization (Kimura: Para [0056] Last sentence).

an input section for receiving an input of a confirmation result of the displayed information from a user (Kimura: Para [0032]: The authentication input means realize the function of accepting button or other physical human inputs so as to notify the authentication/association processing means whether or not the user who manages the wireless area network grants authorization or rejection after the presence of the authentication-requesting mobile station is notified by the authentication request display means); and

an authentication section for executing processing of verifying or not verifying the authentication with the another communication device in accordance with the result input to the input section, and for, when the result is indicative of verification of the authentication, performing key exchange with the another communication device using the device information included in the authentication request and the information included in the authentication response (Kang: Column 3 Line 29 – 33:the client random, the server random and the extracted pre-master secret included in the authentication request / response messages as essential key generation material) & (Kimura: Para [0032]).

As per claim 16, Kang as modified teaches wherein the display section further displays channel information used for reception of the authentication response, in addition to the device information included in the authentication response, thereby making it possible for the user to determine whether or not the authentication response is transferred using another channel by

the unspecified third party (Kang: Column 3 Line 18 – 27, Column 1 Line 49 – 51 and Column 4 Line 35 – 38: a simple ***hash value*** is used for assuring message data integrity (i.e. data is not altered) by using a simple public key).

6. Claim 18 is rejected under 35 U.S.C. 103(a) as being unpatentable over Kang et al. (U.S. Patent 7,096,352), in view of Kimura (U.S. Patent 2001/0048744), and in view of Briscoe et al. (U.S. Patent 7,464,402).

As per claim 18, Kang as modified teaches whether or not a public key and a signature in the device information included in the authentication response are changed, whether or not the received authentication response is changed by the unspecified third party (Kang: Column 3 Line 18 – 27, Column 1 Line 49 – 51 and Column 4 Line 35 – 38: a simple ***hash value*** is used for assuring message data integrity (i.e. data is not altered) by using a simple public key).

However, Kang as modified does not disclose expressly the user is able to determine, based on whether or not the authentication response is received a plurality of times.

Briscoe teaches the user is able to determine, based on whether or not the authentication response is received a plurality of times (Briscoe: Column 7 Line 46 – 48: detect the security against flooding of the network messages).

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Briscoe within the system of Kang as modified because (a) Kang teaches a mutual authentication (co-equal) mechanism between a sender and a receiver (i.e. a client and the server) and allowing a challenge request of receiver authentication to the sender (Kang: Column 2 Line 64 – 65, Column 2 Line 60 – 62 and Column 1 Line 49 – 51), and (b) Briscoe teaches an enhanced security mechanism of detecting the

security against flooding of the network messages (Briscoe: Column 7 Line 46 – 48: detect the security against flooding of the network messages).

Examiner notes: As per claim 11 – 14 and 19 – 26, the claim limitations encompass the similar scopes at least as recited in combining the features from Claims 1 – 2 and 15 – 18 and thus please refer to the same rationale of rejections as set forth above.

Conclusion

Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to LONGBIT CHAI whose telephone number is (571)272-3788. The examiner can normally be reached on Monday-Friday 9:00am-5:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Y. Vu can be reached on 571-272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Longbit Chai/

Primary Examiner, Art Unit 2431
3/2/2009